PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant:	**Richard BROWN et al.**	Examiner:	Thanhnga B TRUONG
Serial No.:	**10/080,477**	Art Unit:	2135
Filed:	February 22, 2002	Our Ref:	B-4518 619564-1 30006602-2 US
For:	"TRUSTED COMPUTING ENVIRONMENT"	Date:	September 27, 2007
		Re:	***Appeal to the Board of Appeals***

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an appeal from the non-Final rejection, dated May 4, 2007, for the above identified patent application. Appellants submit that this Appeal Brief is being timely filed because the Notice of Appeal was filed on August 6, 2007. The amount of $500.00 for the fee set forth in 37 C.F.R. 1.17(c) for submitting this Brief was previously paid in connection with the Appeal Brief filed on June 8, 2006.

REAL PARTY IN INTEREST

The real party in interest to the present application is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

RELATED APPEALS AND INTERFERENCES

There are no other appeals or interferences related to the present application.

STATUS OF CLAIMS

Claims 1 - 18 are pending in the application, stand rejected, are the subject of this Appeal, and are reproduced in the accompanying appendix.

STATUS OF AMENDMENTS

No Amendment After Final Rejection has been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

The invention described and claimed in the present application relates generally to establishing and maintaining a trusted computing environment (p. 1 l. 8). More specifically, a trusted computing network or environment can be established or maintained without a computing device being required to directly challenge the trustworthiness of another device when it is required to communicate with that device (p. 6 ll. 8-10).

Claim 1 in particular is directed to a method of operating a trusted computing system comprising a plurality of computing devices on a network, the method comprising an assessor computing device receiving via the network a report from, and pertaining to the trustworthiness of, a first computing device (p. 5 ll. 19-22 and ll. 27-29), and the assessor computing device updating via the network the trust policy of a second computing device in accordance with the report (p. 5 ll. 22-25 and p. 5 l. 30 – p. 6 l. 6).

Claim 9 is directed to a method of operating a trusted computing system comprising a plurality of computing devices on a network, in which a first computing device has a trusted component (p. 4 ll. 5-6) which issues a report pertaining to the trustworthiness of the first computing device (p. 4 ll. 19-21) wherein a trust policy controller receives said report via the network from the trusted component and updates via the network the trust policy of a second computing device in accordance with said report (p. 5 ll. 22-25 and p. 5 l. 30 – p. 6 l. 6).

Claim 10 is directed to a method of operating a trusted computing system comprising multiple computing devices on a network, the method comprising a trust policy controller receiving reports via the network pertaining to the trustworthiness of each said computing device (p. 4 ll. 6-17), and the trust policy controller determining the trust policy for each of said computing devices in accordance with the trustworthiness of other of said multiple computing devices as determined from said received reports (p. 4 ll. 19-23, p. 5 ll. 22-25 and p. 5 l. 30 – p. 6 l. 6).

Claim 11 is directed to an assessor computing device for controlling a trusted computing system comprising multiple computing devices on a network, the assessor comprising a receiver for receiving via the network a report from, and pertaining to the trustworthiness of, a first computing device (p. 3 l. 29 – p. 4 l. 7 and p. 4 ll. 19-21), an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device via the network (p. 5 ll. 19-25).

Claim 16 is directed to a system comprising an assessor computing device for controlling a trusted computing system comprising multiple computing devices on a network, the assessor comprising a receiver for receiving via the network a report from, and pertaining to the trustworthiness of, a first computing device (p. 3 l. 29 – p. 4 l. 7 and p. 4 ll. 19-21); an updater for updating the trust policy of a second computing device in accordance with the report; and a transmitter for transmitting the updated policy to the second computing device (p. 5 ll. 19-25). The system further comprises first and second computing devices, wherein at least the first computing device comprises a reporter for sending via the network a trustworthiness report to the assessor computing device and at least the second computing device comprises a memory maintaining a trust policy such that the trust policy is modifiable by the transmitter (p. 3 l. 27 – p. 4 l. 3).

Claim 18 is directed to a system comprising multiple computing devices on a network, and a trust policy controller which serves to determine the trust policy of said computing devices (p. 3 l. 27 – p. 4 l. 3). Each of the computing devices has associated with it a trust policy memory to store a trust policy for that computing device, and a trusted component which issues a report pertaining to the trustworthiness of that computing device (p. 4 ll. 5-23, p. 5 ll. 1-7), wherein the controller receives via the network reports from the trust components and updates via the network the trust policy in the trust policy memory of each computing device in accordance with the trustworthiness of other of the multiple computing devices as determined from the reports (p. 5 ll. 22-25 and p. 5 l. 30 – p. 6 l. 6).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1: Whether claims 1-18 are unpatentable under 35 U.S.C. 103(a) over U.S. Pat. No. 6,539,425 to Stevens et al (hereinafter "Stevens") in view of U.S. Pat. No. 5,706,431 to Otto (hereinafter "Otto").

ARGUMENT

Issue 1: Whether claims 1-18 are unpatentable under 35 U.S.C. 103(a) over U.S. Pat. No. 6,539,425 to Stevens et al (hereinafter "Stevens") in view of U.S. Pat. No. 5,706,431 to Otto (hereinafter "Otto").

In section 6a of the Office Action of May 4, the Examiner broadly and in one fell swoop rejects all pending claims 1-18 under 35 U.S.C. 103(a) as being unpatentable over Stevens in view of Otto by, once again, simply cutting-and-pasting the block of text from col. 13 line 54 to col. 14 line 15 of Stevens adjacent to the text of claim 1 and offering nothing more by way of an explanation beyond throwing an "i.e." between the two passages. The Examiner further notes that "Stevens is silent on the capability of updating the report via the network" but finds that "Otto teaches this limitation on column 8, lines 40-47 and line 63 through column 9, line 11; and see also Figure 5, element 110 of Otto" and conveniently but cryptically finds that it would have been obvious to the skilled person to "have modified the invention of Stevens with the teaching of Otto for distributing updates to nodes of a hierarchical communications network that cascade the updates through the network as a function of its hierarchy" and that said skilled person "would have been motivated to have modified the invention of Stevens with the teaching of Otto for propagating revisions through a communications network, wherein the communications network includes a plurality of associated nodes." Applicants respectfully submit that none of the Examiner's proffered "reasons" are in the least bit probative of the alleged obviousness of the present claims.

In their previous reply of February 2, 2007, Appellants noted that the Examiner's "discussion" is beyond inadequate and in clear and complete violation of the unambiguous requirements of 37 C.F.R. §1.104(c)(2) that "the examiner must cite the best references at his or her command. When a reference is complex or shows or describes inventions other than that claimed by Applicant, **the particular part relied on must be designated as nearly as practicable**. The pertinence, if not apparent, must be clearly explained and each rejected claim specified."

Given the complete lack of specificity on the Examiner's part as to what specific element in Stevens is alleged to anticipate which element of the claims, Appellants could in all good faith do no more to reply than to provide what guidance they could to aid the Examiner in his quest to meet the requirements of 37 C.F.R. §1.104(c)(2), questions which are now reiterated below for the Board's benefit:

(1) What exact element in Stevens does the Examiner allege to correspond to the presently claimed assessor computing device?

(2) What exact element in Stevens does the Examiner allege to correspond to the presently claimed first computing device?

(3) What exact element in Stevens does the Examiner allege to correspond to the presently claimed second computing device?

(4) What exact element in Stevens does the Examiner allege to correspond to the presently claimed report received from, and pertaining to the trustworthiness of, a first computing device?

(5) What exact element in Stevens does the Examiner allege to correspond to the presently claimed trust policy of a second computing device?

(6) What exact action in Stevens does the Examiner allege to correspond to the presently claimed assessor computing device updating the trust policy of a second computing device in accordance with the report?

Appellants noted that absent the Examiner answering each of the above questions, Appellants could not possibly provide a reasoned reply without essentially guessing at the

Examiner's interpretation of Stevens and then arguing against that guess – an unfair and unreasonable burden on Appellants.

As the keen reader will no doubt have realized, there is absolutely not the slightest whiff of an answer to any of the above questions in the Examiner's latest action either, thereby prompting the present appeal.

Once again in a good faith effort to assist the prosecution of this application in any way possible, Appellants have nonetheless taken their best guess at what the Examiner *might* be thinking. The essence of the invention of claim 1 is that one computing device (the assessor) receives a report from another computing device (first device) about the trustworthiness of that selfsame (first) device and then updates a trust policy of yet another computing device (the second device) in accordance with the trustworthiness report of the first device that was received from the first device. Stevens discloses storing policy information and executables at individual devices on a network instead of in replicated directory servers arranged in a hierarchical directory structure. The updating of policy information is described as consisting of a network device updating <u>its own policy</u> and possibly the policies of other, peer/colleague devices. Furthermore, the policies discussed by Stevens have nothing to do with trustworthiness of individual computing devices on the network but rather are directed exclusively to <u>network configuration</u> policies – this is made beyond clear all throughout Stevens, from the abstract all the way through the claims.

Thus, Appellants' best and most reasonable guess at interpreting the Examiner's assertion that Stevens discloses all but one limitation of claim 1 is that the Examiner equates the "network configuration policy information" of Stevens with the presently claimed "report pertaining to the trustworthiness of a computing device." If this is correct, the Examiner is clearly - and completely - ignoring a main novelty crux of the invention by (Appellants guess) viewing both the trustiness report and the network configuration policy as just data files. Appellants cannot fathom any other, more reasonable interpretation of the claims and the reference that would lead one to equate a report pertaining to the trustworthiness of a computing device with a network configuration policy information, and respectfully submit to the Board that even this interpretation clearly devoid of any merit.

Furthermore, and regardless, Stevens very clearly teaches that a network device updates its own policy, not the policy of another device in accordance with a trustworthiness report received from yet another device. At best, the device of Stevens updates itself and another device - but not in accordance with a policy received from another device but in accordance with its own policy updating.

The Examiner's assertion of Otto is similarly irrelevant, as Otto teaches simply that information stored at a server (110) on a hierarchical network may be propagated from the server to a client (120) on the network in response to a status report sent by the client to the server. "The status report represents the current status of client node 120a information, and may suitably include an identifier to identify various client node information, a version number associated with various client node information, a revision date associated with various client node information, or the like." (Otto col. 8 ll. 30-36) There is clearly nothing in Otto that has even the most tenuous connection to the presently claimed report pertaining to the trustworthiness of a computing device. All that Otto teaches is a particular method of updating information stored at network nodes via the network - but then Stevens already teaches as much himself in the very portion of his specification cited by the Examiner, and attempting to modify Stevens with Otto as asserted by the Examiner would in fact bring the skilled person no closer to stumbling upon the presently claimed invention.

"To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success... The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, and not based on applicant's disclosure. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations." MPEP §2142.

As set forth above, the Examiner has failed to meet the last prong of the obviousness test set forth in the MPEP as most of the claimed limitations are in fact nowhere to be found in either reference. The Examiner has further failed to meet the first two prongs as well. The Examiner asserts in the last rejection that it would have been obvious to the skilled person to "have modified the invention of Stevens with the teaching of Otto for distributing updates to nodes of a hierarchical communications network that cascade the updates through the network as a function of its hierarchy" and that the skilled person "would have been motivated to have modified the invention of Stevens with the teaching of Otto for propagating revisions through a communications network, wherein the communications network includes a plurality of associated nodes." Conspicuously absent from the Examiner's assertions is any allusion as to **why** the skilled person would be (a) motivated to so modify the invention of Stevens, and (b) have a reasonable expectation of success if attempting such a modification. The burden imposed by the Rules is clear and specific, and the Examiner has failed to meet it. This, of course, is very much the *modus operandi* of the Examiner, which has already resulted in an appeal on which the Examiner was overturned, and which has needlessly necessitated the present and second appeal in this matter. As set forth once before, Appellants are again left with nothing to respond to and can but respectfully ask the Appeals Board to consider their arguments as advanced above and once again overturn the Examiner on appeal.

Appellants submit that the above discussion is equally applicable to all pending claims and thus, in view of all of the preceding, Appellants respectfully submit that all pending claims as presented are novel and nonobvious over the art of record and that the Examiner's rejection is not in compliance with the Rules nor supported by the art, and thus request that the rejection of all claims be overturned on appeal and the case be passed to allowance.

CONCLUSION

For the extensive reasons advanced above, Appellants respectfully contend that each claim is patentable. Therefore, reversal of all rejections and allowance of the case is respectfully solicited.

I hereby certify that this document is being transmitted to the Patent and Trademark Office via electronic filing.

September 27, 2007
(Date of Transmission)

Respectfully submitted,

Robert Popa

Robert Popa
Attorney for Appellants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@la.ladas.com

Attachments

Claims

1. A method of operating a trusted computing system comprising a plurality of computing devices on a network, the method comprising:

an assessor computing device receiving via the network a report from, and pertaining to the trustworthiness of, a first computing device; and

the assessor computing device updating via the network the trust policy of a second computing device in accordance with the report.

2. A method according to claim 1, wherein the assessor computing device updates via the network the trust policies of multiple computing devices in accordance with the report.

3. A method according to claim 1, wherein the assessor computing device updates via the network policies by assessing the trustworthiness of the first computing device on the basis of information about the first computing device in the report.

4. A method according to claim 1, wherein the assessor computing device updates via the network policies on the basis of an assessment of the trustworthiness of the first computing device contained in the report.

5. A method according to claim 1, wherein the assessor computing device requests via the network the first computing device to make the report.

6. A method according to claim 1, wherein the first computing device is caused to report by being started-up or reset, or by an undesirable event occurring.

7. A method according to claim 1, wherein the first computing device is caused to report periodically.

8. A method according to claim 1 in which the second computing device authenticates the trust policy update issued by the assessor computing device before accepting it.

9. A method of operating a trusted computing system comprising a plurality of computing devices on a network, in which a first computing device has a trusted component which issues a report pertaining to the trustworthiness of the first computing device wherein a trust policy controller receives said report via the network from the trusted component and updates via the network the trust policy of a second computing device in accordance with said report.

10. A method of operating a trusted computing system comprising multiple computing devices on a network, the method comprising:

a trust policy controller receiving reports via the network pertaining to the trustworthiness of each said computing device; and

the trust policy controller determining the trust policy for each of said computing devices in accordance with the trustworthiness of other of said multiple computing devices as determined from said received reports.

11. An assessor computing device for controlling a trusted computing system comprising

multiple computing devices on a network, the assessor comprising a receiver for receiving via the network a report from, and pertaining to the trustworthiness of, a first computing device, an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device via the network.

12. An assessor computing device according to claim 11, wherein the updater is arranged to update the trust policies of multiple computing devices in accordance with the report and the transmitter is arranged to transmit the updated policies to the multiple computing devices via the network.

13. An assessor computing device according to claim 11, wherein the updater updates policies by assessing the trustworthiness of the first computing device on the basis of information about the first computing device in the report.

14. An assessor computing device according to claim 11, wherein the updater updates policies on the basis of an assessment of the trustworthiness of the first computing device contained in the report.

15. An assessor computing device according to claim 11 further comprising a requestor, for requesting the report from the first computing device.

16. A system, comprising:

an assessor computing device for controlling a trusted computing system comprising multiple computing devices on a network, the assessor comprising a receiver for receiving via the network a report from, and pertaining to the trustworthiness of, a first computing device,

an updater for updating the trust policy of a second computing device in accordance with the report, and

a transmitter for transmitting the updated policy to the second computing device, and

the system further comprising first and second computing devices, wherein at least the first computing device comprises a reporter for sending via the network a trustworthiness report to the assessor computing device and at least the second computing device comprises a memory maintaining a trust policy such that the trust policy is modifiable by the transmitter.

17. A system as claimed in claim 16 in which the reporter comprises a trusted component associated with the first computing device.

18. A system, comprising:

multiple computing devices on a network, and

a trust policy controller which serves to determine the trust policy of said computing devices;

each of said computing devices having associated with it a trust policy memory to store a trust policy for that computing device, and a trusted component which issues a report pertaining to the trustworthiness of that computing device; wherein

the controller receives via the network reports from the trust components and updates via the network the trust policy in the trust policy memory of each computing device in accordance with the trustworthiness of other of said multiple computing devices as determined from said reports.

There is no evidence submitted with the present Brief on Appeal.

There are no other appeals or interferences related to the present application.